©(ORGANISATION NAME)

CHANGE MANAGEMENT POLICY

Subject: Change Management Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 14	Authorised by:
Effective Date: June 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 INTRODUCTION

The purpose of change management is to increase awareness and understanding of proposed changes across an Organisation and ensure that all changes are made in a thoughtful way that minimises risk and impact to services and customers.

Risk associated with improper change management process:

Reference	Description of Risk
SAFETag	System instability and downtime
SAFETag	Data loss
SAFETag	Lack of accountability and traceability
SAFETag	Security vulnerabilities
SAFETag	Regulatory non-compliance
SAFETag	Third-party risk

1.1 PURPOSE

The purpose of the Change Management Policy is to ensure that changes to Organisation's IT infrastructure are implemented in a controlled and consistent manner, thereby minimising the adverse effect of change related incidents, and consequently improving day-to-day operations.

Changes require adequate forethought, careful monitoring, and follow-up evaluation to reduce impact on IT operations, end users, and other relevant stakeholders and to increase the reliability of the IT infrastructure.

The purpose of Organisation's Change Management process and procedure is to accomplish the following:

1.1.1 Utilise standardised methods and procedures to process Requests for Change (RFCs) efficiently, effectively and in a timely manner.
1.1.2 Minimise the impact of Change related incidents.
1.1.3 Reduce the number of back-outs and failed changes.
1.1.4 Increase the number of changes Organisation can absorb without adverse impact.
1.1.5 Respond quickly to changing business requirements.
1.1.6 Enable the customer success team to swiftly address customer dissatisfaction.
1.1.7 Allow the business to rapidly respond to changing regulatory and compliance requirements.
1.1.8 Minimise exposure to risk.
1.1.9 NO Change Advisory Board (CAB) approved change should be implemented without:
- A request for change (RFC) being raised via the Change Management Form.
- Approval from the Change Advisory Board.

- An approved, documented plan of the sequence or steps for implementing and releasing the change to production environment. This should be stored in an appropriate place e.g. wiki, shared drive, etc.
- Evidence demonstrating the fact that this change has been tested in a pre-production/staging environment first.
- A rollback/mitigation plan in case of failure.
- A post-change test being documented to check that the change has been successfully applied.

1.2 SCOPE

This policy applies to all business processes, information processing facilities and IT systems within Organisation and includes:

- Organisational changes
- Changes to processes
- Changes in technology
- Changes in vendors or vendor services

2.0 POLICY STATEMENT

Change Management shall be performed in accordance with the established Change Management process and procedure.

2.1 The process and procedures shall cover the following:

- Logged Change Requests.
- Identification, prioritisation, and initiation of change.
- Authorisation of change
- Requirements analysis
- Risk Assessment
- Impact Assessment
- Change approach.
- Change testing.
- User acceptance testing and approval.
- Implementation and release planning
- Documentation
- Change monitoring.
- Change classification parameters (e.g. major, minor, emergency change)

2.2 All change requests shall be logged whether approved or rejected on a standardised central system. The approval of all change requests and the results thereafter shall be documented.

2.3 All requests for change within the Organisation will be documented by creating a new change request. The change request will be completed by the change requestor.

2.4 The change requestor will work to develop a specific justification for the change and identify the impact on IT infrastructure, business operations and budget, as well as technical risks and review specific implementation steps.

2.5 The change requestor will be required to submit a functional test plan that is sufficiently detailed to provide assurance that the change will produce the desired result.

2.6 The Change Management team will assess the urgency and impact of the change on IT infrastructure, end user productivity and budget.

2.7 The Change Management Team will assign specific members and identify appropriate end-user members to complete the change request in a manner that will minimise impact on IT infrastructure and end users. If the change does not perform as expected or causes issues to one or more areas of the production environment, the team will determine if the change should be rolled back, and the production environment returned to its prior stable state.

2.8 A review will be conducted by the Change Management team to formally ensure the change has achieved the desired goals. Post implementation actions may include acceptance, modification, or rolling back the change. The team documents the final disposition of the change as part of the Change Request Documentation.

2.9 A documented audit trail containing relevant information shall always be maintained. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel from the change management team.

2.10 A risk assessment shall be performed prior to any change and depending on the intended outcome, an impact assessment should be performed.

2.11 The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable, consider compliance with legislative requirements and standards.

2.12 All change requests shall be prioritised in terms of business case, urgency, effort required (including cost) and potential impact on operations.

2.13 Changes shall be tested in an isolated, controlled, test environment (where such an environment is feasible) prior to implementation, to minimise the effect on the relevant business process, this helps to assess its impact on operations and security and to verify that only intended and approved changes were made.

2.14 The impact of change on existing Service Level Agreements (SLA) shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments, and this should be approved and signed off by relevant parties.

2.15 Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with Record retention policy.

2.16 All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed, and proposed changes were tested.

2.17 All users that would be potentially affected by the change shall be notified of the change in advance. The user representative(s) shall sign off on the change. Users shall be required to make submissions and comments prior to the acceptance of the change.

2.18 Implementation will only be undertaken after appropriate testing and approval by all relevant stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to the effort required to develop and implement the said changes.

2.19 Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change vary from the expected result (as identified during change testing), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Roll back procedures will be in place to ensure the change can be reverted.

2.20 Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the Record retention policy. Policies and procedures, affected by software changes, shall be updated on completion of each change.

2.21 Business continuity plans (BCPs) shall be updated with relevant changes and managed through the change control process. Business continuity plans rely on the completeness, accuracy, and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of an incident or a disaster.

2.22 Specific procedures to ensure proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as emergency changes.

2.23 All changes will be monitored once they have been rolled out to production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

3.0 INFORMATION TECHNOLOGY CHANGES

Change records are kept using the Change Management Form (CMF) as in Appendix A. The following are additional information for Technology Change Management:

3.1 IT staff or other designated employees who are updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes to be made.

3.2 Such changes must be tracked using the Change Management Form – CMF (See Appendix A).

3.3 The employee implementing the change will initiate the change by completing the CMF with a description of changes to be made as required on the form. The impact of such changes shall also be tracked.

3.4 Supervisor/HOD must review before signing the filled CMF.

3.5 The change management team shall also review and approve the changes after the risk assessment has been carried out.
3.6 All necessary data backups must be performed prior to the change.
3.7 There shall be a rollback plan in place to mitigate risks. The employee implementing the change shall also be familiar with the rollback process if the change causes an adverse effect within the system and needs to be reverted.

4.0 CATEGORIES OF CHANGE

To decide which route a change should take through the process, change requests will be categorised based on its estimated resource requirement, urgency, and risk.

The following categories of change will be used:

4.1 STANDARD CHANGE

A standard change is a small, low risk change that can be implemented in a short, governed timeframe. Although a standard change is technically a change, it will not require a change request to be assessed and approved, although it should still be logged against the relevant configuration item as having taken place.

Some standard changes will be requested by users via the service request process. This will be subject to specifically agreed target service levels specified in the SLA.

4.2 NORMAL CHANGE

A normal change is one which has not been pre-classified as a standard change, is not an emergency and does not meet the criteria for a major change. Normal changes will be subject to the change management process.

4.3 EMERGENCY CHANGE

Emergency changes are changes which are urgently required to resolve a major incident or problem. These will be fast-tracked through the change management process and given additional resources where required. Note that a failure in forward planning to log a normal change in timely to obtain approval does not constitute an emergency change and will not be treated as such.

4.4 MAJOR CHANGE

Changes with a potential of having a major impact on a service, although still logged as change requests and tracked via the change management process, should be handled via a Design and Transition of New or Changed Services process.

5.0 RECOMMENDATIONS/ ADVISORY ON CHANGE MANAGEMENT

Organisations with 1 – 5 Employees	Organisations with 6 – 20 Employees	Organisations with more than 20 Employees
• Make use of shared documents or spreadsheets (e.g., Google Docs or Sheets) to track and document changes. • Implement a basic approval process using email or messaging tools (e.g., Slack, Microsoft Teams) for peer reviews and approvals. • Leverage cloud-based project management tools like Trello https://trello.com/ Asana https://asana.com/ or Zoho project https://www.zoho.com/ to manage change requests, assign tasks, and track progress. • Utilise version control systems like Git https://git-scm.com/ for tracking and managing changes to code or configuration files.	• Implement a change management software like Cherwell Service Management https://www.cherwell.com/ or ServiceNow https://www.servicenow.com/ to streamline the entire change management lifecycle, including request submission, approval workflows, and reporting. • Use a configuration management database (CMDB) like SolarWinds Service Desk https://www.solarwinds.com/service-desk. or Axios Assyst https://www.axiossystems.com/ to maintain an inventory of IT assets and track their configurations. • Adopt a project portfolio management (PPM) tool like Planview https://www.planview.com/ or to prioritise and coordinate changes alongside other projects and initiatives. • Leverage collaboration and knowledge-sharing	• Implement an enterprise change management solution like BMC Helix ITSM https://www.bmc.com/it-solutions/bmc-helix-itsm.html or ServiceNow https://www.servicenow.com/ to manage the entire change management lifecycle, including advanced features like risk assessments, impact analysis, and compliance reporting. • Integrate with other IT service management (ITSM) processes like incident management, problem management, and release management using tools like Cherwell Service Management https://www.cherwell.com/. • Implement a robust configuration management database (CMDB) like ServiceNow CMDB https://www.servicenow.com/products/servicenowplatform/configuration-management-database.html

	platforms like Confluence https://www.atlassian.com/software/confluence to document processes, share best practices, and facilitate team collaboration.	or BMC Atrium CMDB https://www.bmc.com/it-solutions/atrium-cmdb.html to maintain a centralised repository of IT assets and their relationships. • Leverage enterprise collaboration and knowledge management platforms: Microsoft SharePoint https://www.microsoft.com/en-us/microsoft-365/sharepoint/collaboration to facilitate team collaboration, document sharing, and knowledge management.

Appendix A

- Refer to change management form.

APPENDIX A: CHANGE REQUEST FORM FOR CHANGE MANAGEMENT

Change Request Form

Date:	
Name of person originating request:	
Change Request – Description of change	
System or information asset (identify all software, information, database entities and hardware that might require amendment) to be changed (target)	
Detail of change(s) required	
Business case/benefits for change (including ROI) if relevant	

Technical case for and against change (include costs and time required and any scheduling issues)	
Risk assessment outcome (i.e. risks identified)	
Impact of Change	
Roll Back Plan	
Priority	
Approval (signature and date)	
Human Resources – Change management Team Managing Director – Change Advisory Board	Signature: DD/MM/YYYY
Date Allocated	DD/MM/YYYY

Date Completed	DD/MM/YYYY